REMARKS

This Amendment is a submission under 37 C.F.R. § 1.114 for a Request for Continued Examination (RCE).

In the Office Action, claims 1-2, 4 and 7-22 were rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent 6,182,216 (Luyster) in view of U.S. Patent 5,317,639 (Mittenthal). The Examiner also stated that deterministically generating maximal nonlinear block substitution tables is not patentable as there have been disclosures of using linear orthomorphisms to create nonlinear block substitution tables. The Examiner also cited MPEP § 2144.05 for the proposition that optimizing an algorithm will not support the patentability of subject matter encompassed by the prior art unless there is evidence indicating such optimization is critical.

For at least the reasons set forth hereinbelow, Applicants request that the rejections associated with the pending claims be withdrawn.

Corrections/Clarifications

1. Paragraph 5 of the Office Action erroneously states that a feature of the applicant's invention relied on by the applicant is that the nonlinear orthomorphisms do not possess the property of lack of mutual information. **First**, nonlinear orthomorphisms do posses the property of lack of mutual information, a unique property that is a characterization of all orthomorphisms, both linear and nonlinear. **Second**, the references to the property of lack of mutual information made by Applicant in the previous responses were to clarify that the maximal nonlinear block substitution tables recited in claim 1 are not orthomorphisms, and therefore could not possibly be anticipated by the previously cited Mittenthal references.

2. Paragraph 6 of the Office Action states that deterministically generating maximal nonlinear block substitution tables is not patentable as there have been disclosures of using linear orthomorphisms to create nonlinear block substitution tables. **First**, Applicant notes that the Examiner has not identified which disclosures do so. **Second**, if the Examiner is referring to the Mittenthal patent (the '639 patent), Applicant submits that the '639 patent discloses using pairs of linear orthomorphisms to create nonlinear orthomorphisms for block substitution tables – not block substitution tables having maximal nonlinearity. **Third**, Applicant notes that the Examiner is not asserting that there have been disclosures of combining linear orthomorphisms to create maximal nonlinear block substitution tables as recited in claim 1 of this application. In fact, all of the references cited by the Examiner fall well short of achieving block substitution tables having maximal nonlinearity.

3. Paragraph 6 of the Office Action erroneously states that no evidence has been provided that such an optimization (maximal nonlinearity) is critical or produces unexpected results. **First**, Applicant submits that one skilled in the art would readily acknowledge that maximal nonlinearity is one of the most sought after properties in block substitutions. Both the government and private industry are seeking methods of consistently producing highly nonlinear and/or maximal nonlinear block substitution tables. **Second**, Applicant notes that lines 14-29 of page 1 of the specification clearly set forth the importance of block substitution tables that are highly nonlinear, and by implication, the importance of block substitution tables that have maximal nonlinearity (e.g., a principal foil against differential and linear cryptanalysis). **Third**, at the time this application was filed, the accepted method of generating block substitution tables having any nonlinearity was to employ exhaustive random searching and extensive testing. Many in the cryptographic community

did not believe that block substitution tables having maximal nonlinearity could be generated deterministically. Therefore, Applicant respectfully submits that the results produced by the recited method (i.e., block substitution tables having maximal nonlinearity) were certainly unexpected. As recently as August 2004, some practicioners in the cryptographic community still remained skeptical that the nonlinear mapping technique disclosed in the application could really provide the maximal nonlinearity.

4. Paragraph 26 of the Office Action states that Luyster teaches selecting pairs of cycles from the first and second linear orthomorphisms to produce a mapping for which N(x,y)!=0 for all pairs of numbers from different cycles. According to this equation, if N!=0, then N(x,y)=0. Therefore, the assertion that Luyster teaches selecting pairs of cycles from the first and second linear orthomorphisms to produce a mapping for which N(x,y)!=0 for all pairs of numbers from different cycles is simply a statement that the Luyster patent produces only linear mappings – not the nonlinear mappings produced by the method recited in the present application.

Claims 1-2, 4 and 7-15

Claim 1 recites a method of **deterministically** generating **maximal** nonlinear block substitution tables for a predetermined block size. The method includes, among other things, creating **maximal** nonlinear block substitution tables by combining linear orthomorphisms.

Applicant submits that independent claim 1 is nonobvious over the combination of Luyster and Mittenthal because the cited references fail to teach or suggest each and every element of claim 1. *See* MPEP § 2143 (stating that one of the elements of a *prima facie* case of obviousness under § 103(a) is that the prior art references, either alone or in combination, must teach or suggest every limitation of the claimed invention). More particularly, Applicant submits that the cited references fail to teach or suggest a method that includes, among other things, deterministically generating maximal nonlinear block substitution tables for a predetermined block size by "creating maximal nonlinear block substitution tables by combining the linear orthomorphisms" as recited in claim 1.

As explained previously, Applicant submits that Luyster merely teaches or suggests information relating to the inter-round mixing process used in some encryption techniques. Thus, although Applicant respectfully disagrees with many of the Examiner's determinations concerning the teachings of Luyster, Applicant agrees with the Examiner's determination that Luyster fails to teach or suggest creating **maximal** non-linear block substitution tables as recited in claim 1.

As explained hereinabove, Applicant also submits that Mittenthal (the '639 patent) discloses using pairs of linear orthomorphisms to create nonlinear orthomorphisms for block substitution tables – not block substitution tables having maximal nonlinearity. The nonlinearity achieved by the '639 patent was relatively small and fell well short of achieving block substitution tables having high nonlinearity, let alone maximal linearity.

Thus, Applicant respectfully submits that it would not have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Luyster and Mittenthal (the '639 patent) to produce the invention recited in claim 1.

Therefore, for at least the reasons stated hereinabove, Applicant submits that claim 1 is nonobvious over the combination of Luyster and Mittenthal (the '639 patent) because the cited references fail to teach or suggest each and every element of claim 1. *See* MPEP § 2143 *id.* Applicant further submits that claims 1-2, 4 and 7-15, which depend from claim 1, are also nonobvious over the combination of Luyster and Mittenthal (the '639 patent). *See* MPEP § 2143.03 (stating that if an independent claim is nonobvious under §103(a), then any claim depending therefrom is nonobvious). Accordingly, Applicant respectfully requests that the rejections associated with claims 1-2, 4 and 7-15 be withdrawn.

Claims 16-17

Applicant submits that independent claim 16 is nonobvious over the combination of Luyster and Mittenthal because the cited references fail to teach or suggest each and every element of claim 16. *See* MPEP § 2143 *id.* More particularly, Applicant submits that the cited references fail to teach or suggest, among other things, "setting the maximal nonlinear block substitution tables based on a combination of the linear orthomorphisms, the substitution tables for use in encrypting clear text messages which are in the form of a sequence of binary numbers" as recited in claim 16.

For at least reasons similar to those set forth hereinabove, Applicant submits that claim 16 is nonobvious over the cited references. *See* MPEP § 2143 *id.* Applicant further submits that claim17, which depends from claim 16, is also nonobvious over the cited references. *See* MPEP § 2143.03 *id.* Accordingly, Applicant respectfully requests that the rejections associated with claims 16 and 17 be withdrawn.

Claims 18-19

Applicant submits that independent claim 18 is nonobvious over the combination of Luyster and Mittenthal because the cited references fail to teach or suggest each and every element of claim 18. *See* MPEP § 2143 *id.* More particularly, Applicant submits that the cited references fail to teach or suggest, among other things, "setting the maximal nonlinear block substitution tables by combining the linear orthomorphisms, the substitution tables for use in encrypting clear text messages which are in the form of an ordering of binary numbers" as recited in claim 18.

For at least reasons similar to those set forth hereinabove, Applicant submits that claim 18 is nonobvious over the cited references. *See* MPEP § 2143 *id.* Applicant further submits that claim19, which depends from claim 18, is also nonobvious over the cited references. *See* MPEP § 2143.03 *id.* Accordingly, Applicant respectfully requests that the §103(a) rejections associated with claims 18 and 19 be withdrawn.

Claims 20, 21 and 22

For at least reasons similar to those set forth hereinabove, Applicant submits that independent claims 20, 21 and 22 are nonobvious over the combination of Luyster and Mittenthal (the '639 patent) because the cited references fail to teach or suggest each and every element of these claims. *See* MPEP § 2143 *id.* Accordingly, Applicant respectfully requests that the rejections associated with claims 20, 21 and 22 be withdrawn.

CONCLUSION

Applicants respectfully request a Notice Of Allowance for the pending claims in the present application. If the Examiner is of the opinion that the present application is in condition for disposition other than allowance, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below in order that the Examiner's concerns may be expeditiously addressed.

Respectfully submitted,

Date: March 9, 2005

Robert A Muha
Robert A. Muha
Reg. No. 44,249

KIRKPATRICK & LOCKHART NICHOLSON GRAHAM LLP
Henry W. Oliver Building
535 Smithfield Street
Pittsburgh, Pennsylvania 15222

Telephone:	(412) 355-8244
Facsimile:	(412) 355-6501
E-mail:	rmuha@klng.com